# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-008797
(43)Date of publication of application : 10.01.1997

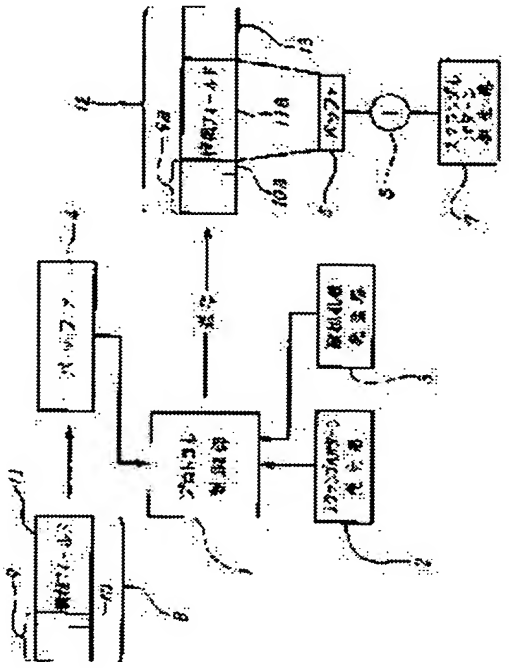
(51)Int.Cl. H04L 9/06
H04L 9/14
G09C 1/00
H04L 12/56

(21)Application number : 07-149036
(22)Date of filing : 15.06.1995

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : KUNO YUTAKA

## (54) SCRAMBLE METHOD

(57)Abstract:
PURPOSE: To disable the decoding of a scramble pattern from the outside even when field lengths on respective transmission and reception sides are not equal by loading scramble after transmissive data for one packet are made full by embedding a pseudo random number sequence in a section after the end of transmissive data.
CONSTITUTION: Transmission data 8 are transmitted by exclusively ORing a bit train generated by a scramble pattern generator 2. When the remaining data of transmission data 8 are less than transmission data for one packet, the excess part of the final packet is filled with the bit string of pseudo random number sent from a pseudo random number generator 3. On the reception side, received data 12 are successively stored in a buffer and only the required part is segmented by watching a field 10a of frame length information, moved to a buffer 5 and outputted by exclusively ORing a bit train generated by a scramble pattern generator 7.



LEGAL STATUS

| | |
|---|---|
| [Date of request for examination] | 16.11.1999 |
| [Date of sending the examiner's decision of rejection] | 20.05.2003 |
| [Kind of final disposal of application other than the examiner's decision of rejection or application converted registration] | |
| [Date of final disposal for application] | |
| [Patent number] | 3627765 |
| [Date of registration] | 17.12.2004 |
| [Number of appeal against examiner's decision of rejection] | 2003-11274 |
| [Date of requesting appeal against examiner's decision of rejection] | 19.06.2003 |
| [Date of extinction of right] | |

* NOTICES *



1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

## CLAIMS

[Claim(s)]
[Claim 1] The scramble approach characterized by to apply a scramble after divide the data A which should be transmitted per a fixed-length packet or frame, and it transmits and receives them, it embeds pseudo-random number sequence into the part after the tail of the before this data A when the packet or the frame containing the bit of the tail of said data A does not fulfill one packet or the transmit data for one frame in the correspondence procedure which performs the information secrecy by scramble in that case, and filling one packet or the transmit data for one frame.
[Claim 2] In the correspondence procedure which divides the data A which should be transmitted per a fixed-length packet or frame, transmits and receives them, and performs the information secrecy by scramble in that case When the packet or frame containing the bit of the tail of said data A does not fulfill one packet or the transmit data for one frame, The scramble approach characterized by applying a scramble after embedding these some data A into the part after the tail of the before this data A and filling one packet or the transmit data for one frame.
[Claim 3] In the correspondence procedure which divides the data A which should be transmitted per a fixed-length packet or frame, transmits and receives them, and performs the information secrecy by scramble in that case When the packet or frame containing the bit of the tail of said data A does not fulfill one packet or the transmit data for one frame, While embedding the character string of "0" or arbitration into the part after the tail of the before this data A and filling one packet or the transmit data for one frame The scramble approach characterized by applying a scramble about the part from the head of the data in this packet or a frame to the tail of Data A.

[Translation done.]

* NOTICES *

JPO and NCIPI are not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

## DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Industrial Application] The frame length of a transmitting side and a receiving side differs especially about transmission of the digital signal in the case of taking an information secrecy method, and this invention relates to the scramble approach that it can prevent that the information concerning information secrecy is revealed,

even when the part to which data do not exist in one frame arises.
[0002]
[Description of the Prior Art] drawing showing the example of the layer configuration (protocol stack) of the communication system of the former [ drawing 5 ] — it is — the figure sign 61 — a header and 61-b express information field and, as for the frame of a high order layer, and 61-a, as for the frame of a lower layer, 62-a, 63-a, and 64-a, a header, 62-b, 63-b, and 64-b express [ 62-64 ] information field, respectively.
[0003] Moreover, the part where the tail of the frame of a high order layer was exhausted by information field 64-b of the frame 64 of a lower layer, and, as for the alpha code B, the information on information field 61-b of the frame 61 of a high order layer was exhausted, as for C, and D express the part in which the information from a high order layer does not exist within information field 64-b of the frame 64 of a lower layer.
[0004] As conventionally shown in drawing 5, when the frame size of a high order layer had not become the multiple of the data length contained in one frame of a lower layer in the communication system which consists of two or more layers, 0 was embedded into the part shown by D after the part C corresponding to the tail of the frame of the high order layer of the frame 64 of the lower layer containing the frame tail C of a high order layer.
[0005] Moreover, also in the communication system which does not take two or more layer configuration, when the die length of the data which a user wants to send had not become the multiple of the data length contained in one frame, 0 was embedded into the part after a data tail like the above-mentioned case.
[0006] Thus, there is "radio equipment of the radio station which performs land-mobile wireless data transmission" (January 25, 1990 decision) specified to one of the systems which embed a frame tail in null code by RCRSTD-6.
[0007]
[Problem(s) to be Solved by the Invention] As an approach of keeping information secret about the data to transmit, the binary ("1" "0") pseudo-random number is generated, and an exclusive OR with data is calculated, it transmits, and the method which decodes by generating the pseudo-random number sequence of the same sequence is taken in a receiving side in many cases.
[0008] Since the train of "0" is included in the tail of one data frame as data a fixed period or each time on conditions from which it is between transmission and reception which were mentioned above, while frame length has not become the integral multiple of the information field of the frame of another side, when the scramble for the above information secrecy is applied, in this part, a scramble pattern and the exclusive OR (i.e., the scramble pattern (pseudo-random number) itself) of "0" will be sent out to a transmission line.
[0009] Drawing 6 is drawing showing the example of a scramble pattern generator. In this drawing, 65-1 to 65-10 shows a register, and 66 shows the exclusive "or" circuit.
[0010] In the system which performs the information secrecy by scramble A scramble pattern generator (it consists of linearity feedback shift registers) as shown in this drawing is used. To a register 65-1 to 65-10 (one stores the data which are 1 bit) Secret ID of a terminal etc. is set, and it shifts the value of a register to one right at a time for every cycle, and outputs 1 bit at a time from a right end register, and a triplet eye and the bit [ 10th ] exclusive OR are inputted into a left end.
[0011] If the structure of a scramble pattern generator is not known, the structure of a part for 2mbit and a scramble pattern generator is known and the pseudo-random number for m bits is known when the number of bits of a scramble pattern generator is set to m, the value of an initial value register can be counted backward by solving simultaneous equations. As one example of the value of m, it is determined by the personal handy phone standard (RCR STD-28) that 10 bits is used.
[0012] Therefore, it was the place where the problem which says the value of the initial value register of a scramble pattern generator presumed by the third person depending on conditions from the contents of the scramble pattern, and which is not desirable is expected.
[0013] This invention is accomplished in order to solve such a conventional technical problem, and even if it is a case which is not equal, it aims at offering the scramble approach which cannot decode a scramble pattern from the exterior.
[0014]
[Means for Solving the Problem] According to this invention, an above-mentioned technical problem is solved by the means indicated to said claim.
[0015] Namely, invention of claim 1 divides the data A which should be transmitted per a fixed-length packet or frame, and transmits and receives them, and it sets to the correspondence procedure which performs the information secrecy by scramble in that case. When the packet or frame containing the bit of the tail of said data

A does not fulfill one packet or the transmit data for one frame, After embedding pseudo-random number sequence into the part after the tail of the before this data A and filling one packet or the transmit data for one frame, it is the scramble approach constituted so that a scramble might be applied.

[0016] In the correspondence procedure which invention of claim 2 divides the data A which should be transmitted per a fixed-length packet or frame, transmits and receives them, and performs the information secrecy by scramble in that case When the packet or frame containing the bit of the tail of said data A does not fulfill one packet or the transmit data for one frame, After embedding these some data A into the part after the tail of the before this data A and filling one packet or the transmit data for one frame, it is the scramble approach constituted so that a scramble might be applied.

[0017] In the correspondence procedure which invention of claim 3 divides the data A which should be transmitted per a fixed-length packet or frame, transmits and receives them, and performs the information secrecy by scramble in that case When the packet or frame containing the bit of the tail of said data A does not fulfill one packet or the transmit data for one frame, While embedding 0 into the part after the tail of the before this data A and filling one packet or the transmit data for one frame, it is the scramble approach constituted so that a scramble might be applied about the part from the head of the data in this packet or a frame to the tail of Data A.

[0018]

[Function] This invention is divided per a fixed-length packet or frame, and transmits and receives data, and a third person takes care not to decode the scramble pattern for information secrecy from transmission data in the communication system constituted so that the information secrecy by scramble might be performed in that case.

[0019] In invention of claim 1, the pseudo-random number sequence is embedded in the null section produced from the difference of a data length, and a packet or frame length. Since this null section was conventionally filled with "0", the scramble had been applied by taking the exclusive OR of "0" and each bit of a scramble pattern.

[0020] Therefore, although the result to which the scramble pattern itself will be transmitted was produced, since it is lost that the scramble pattern itself appears by embedding a pseudo-random number sequence in this way, it can prevent that a scramble pattern is decoded from transmission data by the third person. Therefore, the contents of the initial value register of a scramble pattern generator are not presumed.

[0021] Moreover, in invention of claim 2, the null section in a packet or a frame is embedded using some data instead of a pseudo-random number. Therefore, it can prevent that a scramble pattern is decoded from transmission data by the third person for the same reason as the case of claim 1.

[0022] Furthermore, although the null section in a packet or a frame is filled with the data of "0" or arbitration, he is trying to apply a scramble except for this part in invention of claim 3. Since taking and outputting each bit of a scramble pattern and the exclusive OR of "0" also by this approach is lost, a scramble pattern does not appear outside. Therefore, it can prevent that a scramble pattern is decoded from transmission data by the third person.

[0023]

[Example] drawing where drawing 1 explains the 1st example of this invention — it is — the figure sign 1 — a buffer and 6 express an exclusive "or" circuit and, in a pseudo-random number generator, and 4 and 5, 8 expresses [ a protocol control section, and 2 and 7 / a scramble pattern generator and 3 ] the transmit data and the pseudo-random number sequence to which information field and 12 were added with received data, and 13 was added [ 9 and 9a / a header, and 10 and 10a ] for the field of frame length information, and 11 and 11a by the transmitting side.

[0024] As shown in this drawing, in a transmitting side, the data 8 which had the Request to Send from the user or the high order layer are once stored in a buffer 4, and one batch takes them out transmit data every, and the protocol control section 1 calculates an exclusive OR with the bit string generated by the scramble pattern generator 2, and transmits them.

[0025] When the remaining data of transmit data 8 do not fulfill the transmit data for one frame or 1 packet, the part in which the last frame or the packet remained is fill uped with the bit string of the pseudo-random number sent from the pseudo-random number generator 3.

[0026] The data 12 sent in the receiving side are stored in the buffer (not shown) one by one, field 10a showing frame length is seen, and only a need part is started, it moves to a buffer 5, and an exclusive OR with the bit string generated with the scramble pattern generator 7 is calculated and outputted.

[0027] Drawing 2 is drawing explaining the 2nd example of this invention, and is the same as that of the case of drawing 1 which explained previously about a figure sign. Moreover, since the configuration of a receiving side is the same as that of the case of drawing 1 in general, only the transmitting side shows it in this Fig.
[0028] In this drawing, the data 8 which had the Request to Send from the user or the high order layer are once stored in a buffer 4, and one batch takes them out transmit data every, and the protocol control section 1 calculates an exclusive OR with the bit string generated by the scramble pattern generator 2, and transmits them.
[0029] When the remaining data of transmit data 8 do not fulfill the transmit data for one frame or 1 packet at this time, bit string E of the required die length of the tail of transmit data 8 is reproduced and embedded to the field F after the frame in which the last bit of transmit data 8 is contained, or the bit concerned of a packet, an exclusive OR with the bit string generated by the scramble pattern generator 2 is calculated, and it sends out on a transmission line.
[0030] Drawing 3 is drawing explaining the 3rd example of this invention, and is the same as that of the case of drawing 1 which explained previously about a figure sign. Moreover, since the configuration of a receiving side is the same as that of the case of drawing 1 in general, this Fig. shows only the transmitting side.
[0031] In this drawing, the data 8 which had the Request to Send from the user or the high order layer are once stored in a buffer 4, and the protocol control section 1 calculates an exclusive OR with the bit string which one batch took out the transmit data every and was generated by the scramble pattern generator 2, and they are transmitted.
[0032] When the remaining data of a buffer 4 do not fulfill the transmit data for one frame or 1 packet, a transmitting side looks at the field 10 showing the frame length in the data 8 which had the Request to Send from the user or the high order layer, makes the scramble pattern generator 2 generate the bit string of only a required number, and does not perform scramble processing into the part in which the last frame or the packet remained, but embeds "0", and sends it out to a transmission line. The data which are embedded in the case of this example do not need to be "oar 0", and may be the character string of arbitration.
[0033] Drawing 4 is drawing showing the example of the protocol based on a personal handy phone standard (RCR STD-28). In this drawing, in the figure sign 14, a personal station (PS) and 15 show a cel station (CS), and 16 shows the network (network).
[0034] When performing packet communication based on this specification, as shown in the need of charging to this drawing, it is end because of the confirmation of receipt of data. to Termination is carried out by end. The protocol structure which places a LAPD (Link Access Procedure on the D-channel) layer on the LAPDC (Link Access Procedure for Digital Cordless) layer by which termination is carried out between personal digital assistant-base transceiver stations can be considered.
[0035] In this configuration, when the data Request to Send over two or more LAPD frames occurs, in order to divide, send and receive the LAPD frame (information field a maximum of 260 octet + control section 5 / 6 octet = 2120/2128 bit) on the LAPDC frame (20 octets = 160 bits), the procedure in which a null bit which was explained by the Prior art about 15/14 byte = too much 120/112 bit is fill uped with "0" is performed.
[0036] Thus, in actual communication system, the dependability of information secrecy can be raised by existing mostly, when the procedure in which a null bit which was explained by the Prior art is fill uped with "0" is performed to a bit string 20 bits or more, and applying this invention in such a case, and a scramble pattern being made not to be sent out to a transmission line as it is.
[0037]
[Effect of the Invention] In the communication system which divides the data which should be transmitted per a fixed-length packet or frame, transmits and receives them, and performs the information secrecy by scramble in that case according to this invention as explained above The packet or frame containing the bit of the tail of data which should transmit Since it can prevent detecting a scramble pattern from the bit string after the tail of this transmit data when not fulfilling one packet or the transmit data for one frame A possibility that a third person may presume the value of the initial value register of a scramble pattern generator is abolished, and there is an advantage which can perform positive information secrecy.

---

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

## DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is drawing explaining the 1st example of this invention.
[Drawing 2] It is drawing explaining the 2nd example of this invention.
[Drawing 3] It is drawing explaining the 3rd example of this invention.
[Drawing 4] It is drawing showing the example of the protocol structure of the packet communication based on a personal handy phone standard.
[Drawing 5] It is drawing showing the example of the layer configuration of the conventional communication system.
[Drawing 6] It is drawing showing the example of a scramble pattern generator.
[Description of Notations]
1 Protocol Control Section
2 Seven Scramble pattern generator
3 Pseudo-random Number Generator
4 Five Buffer
6 Exclusive "or" Circuit
8 Transmit Data
9 9a Header
10 10a The field of frame length information
11 11a Information field
12 Received Data
13 Pseudo-random Number Sequence Added by Transmitting Side
14 Personal Station
15 Cel Station
16 Network

[Translation done.]

* NOTICES *

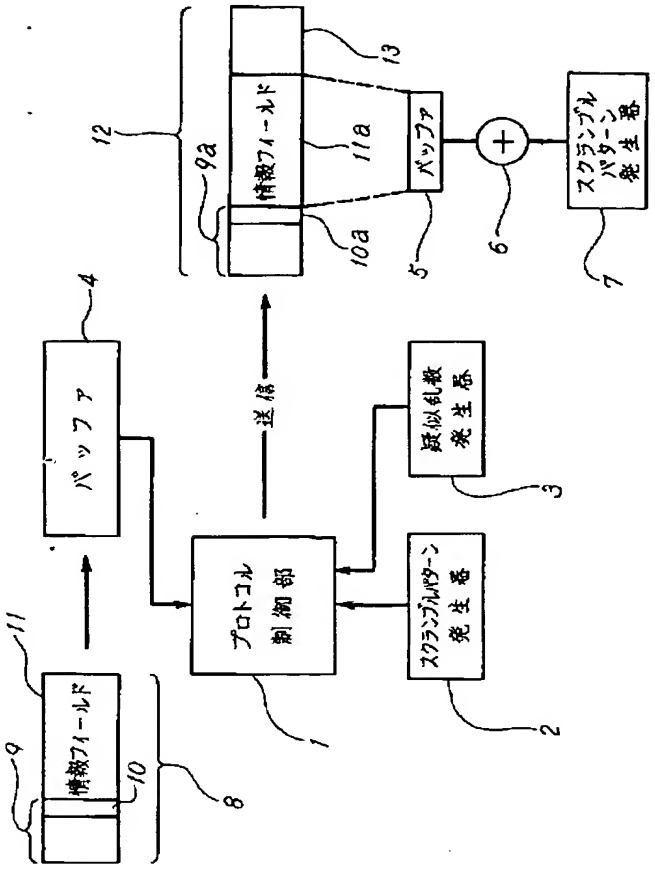
JPO and NCIPI are not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

## DRAWINGS

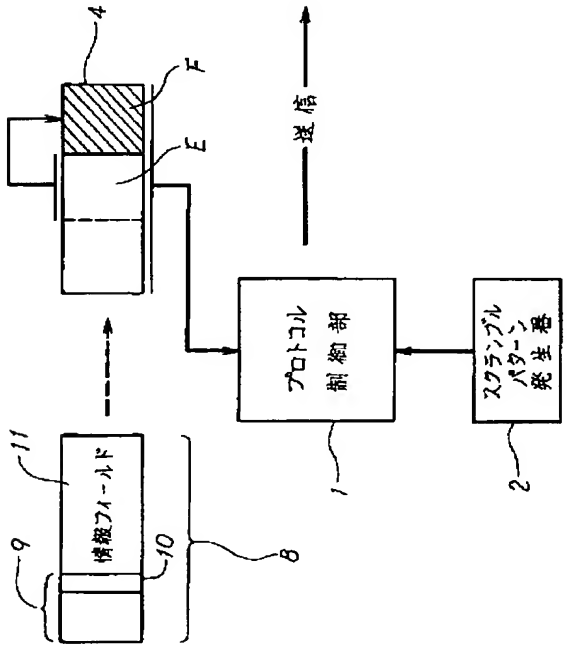
[Drawing 1]

本発明の第1の実施例を説明する図



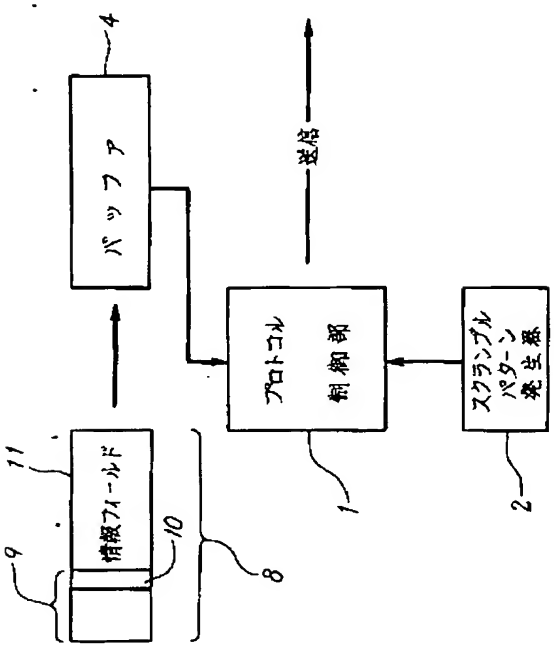

[Drawing 2]

本発明の第2の実施例を説明する図



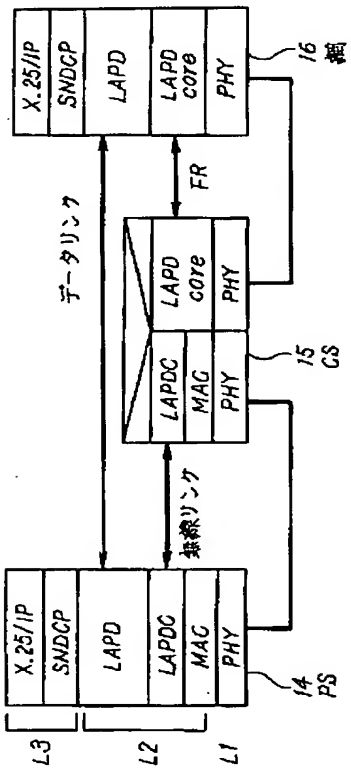

[Drawing 3]

本発明の第3の実施例を説明する図



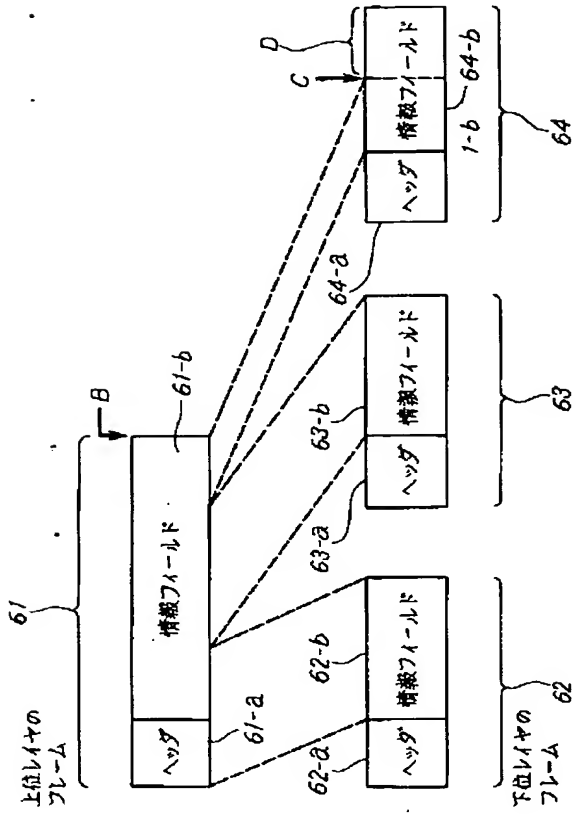

[Drawing 4]

RCR STD-28に準拠したパケット通信のプロトコル構成の例を示す図



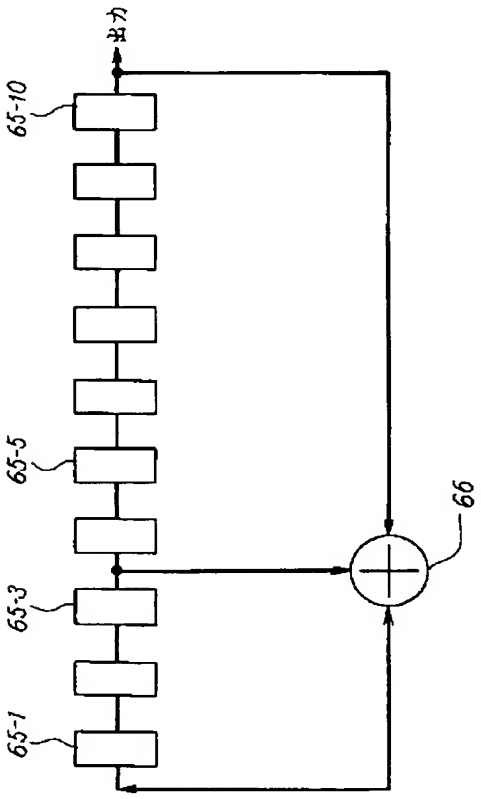

[Drawing 5]

従来の通信システムのレイヤ構成の例を示す図




[Drawing 6]

スクランブルパターン発生器の例を示す図



[Translation done.]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

**特開平9－8797**

(43)公開日　平成９年(1997)１月10日

| (51)Int.Cl.[6] | | 識別記号 | 庁内整理番号 | ＦＩ | | 技術表示箇所 |
|---|---|---|---|---|---|---|
| Ｈ０４Ｌ | 9/06 | | | Ｈ０４Ｌ | 9/02 | Ｚ |
| | 9/14 | | 7259－5Ｊ | Ｇ０９Ｃ | 1/00 | |
| Ｇ０９Ｃ | 1/00 | | 9466－5Ｋ | Ｈ０４Ｌ | 11/20 | １０２Ａ |
| Ｈ０４Ｌ | 12/56 | | | | | |

審査請求　未請求　請求項の数３　ＯＬ　（全 ７ 頁）

(21)出願番号　特願平7－149036

(22)出願日　平成７年(1995)６月15日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号

(72)発明者　久埜　豊
東京都千代田区内幸町一丁目１番６号　日本電信電話株式会社内

(74)代理人　弁理士　本間　崇

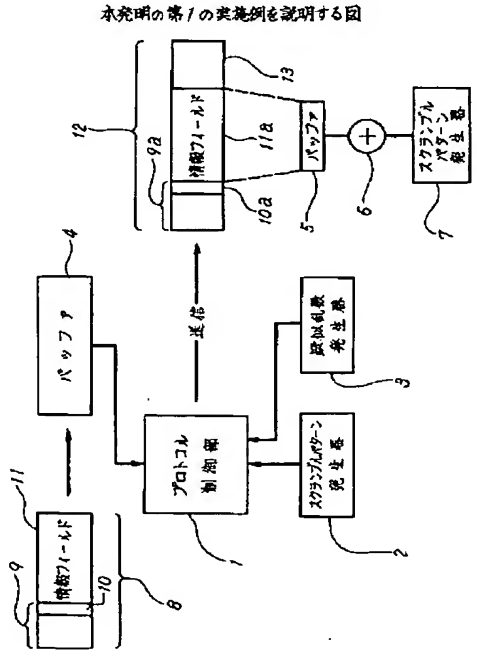
(54)【発明の名称】　スクランブル方法

(57)【要約】

【目的】　ディジタル信号を固定長のパケットあるいはフレームで送受信する場合のスクランブル方法に関し、パケットあるいはフレーム内のデータの末尾以降に送信データが存在しない箇所がある場合でも第三者によるスクランブルパターンの検出を阻止し得る手段の実現を目的とする。

【構成】　送信すべきデータＡを固定長のパケットまたはフレーム単位に分割して送受信し、その際スクランブルによる情報秘匿を行なう通信方法において、前記データＡの末尾のビットを含むパケットまたはフレームが、１パケットまたは１フレーム分の送信データに満たない場合、前該データＡの末尾以降の部分に擬似乱数列を埋め込んで１パケットまたは１フレーム分の送信データを満たしてからスクランブルをかけるように構成する。

本発明の第１の実施例を説明する図



1

【特許請求の範囲】
【請求項１】　送信すべきデータＡを固定長のバケットまたはフレーム単位に分割して送受信し、その際スクランブルによる情報秘匿を行なう通信方法において、
前記データＡの末尾のビットを含むバケットまたはフレームが、１バケットまたは１フレーム分の送信データに満たない場合、前該データＡの末尾以降の部分に擬似乱数列を埋め込んで１バケットまたは１フレーム分の送信データを満たしてからスクランブルをかけることを特徴とするスクランブル方法。
【請求項２】　送信すべきデータＡを固定長のバケットまたはフレーム単位に分割して送受信し、その際スクランブルによる情報秘匿を行なう通信方法において、
前記データＡの末尾のビットを含むバケットまたはフレームが、１バケットまたは１フレーム分の送信データに満たない場合、前該データＡの末尾以降の部分に、該データＡの一部分を埋め込んで１バケットまたは１フレーム分の送信データを満たしてからスクランブルをかけることを特徴とするスクランブル方法。
【請求項３】　送信すべきデータＡを固定長のバケットまたはフレーム単位に分割して送受信し、その際スクランブルによる情報秘匿を行なう通信方法において、
前記データＡの末尾のビットを含むバケットまたはフレームが、１バケットまたは１フレーム分の送信データに満たない場合、前該データＡの末尾以降の部分に“０”または任意の文字列を埋め込んで１バケットまたは１フレーム分の送信データを満たすと共に、該バケットまたはフレーム内のデータの先頭からデータＡの末尾までの部分についてスクランブルをかけることを特徴とするスクランブル方法。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明は、情報秘匿方式を採る場合のディジタル信号の伝送に関し、特に、送信側と受信側とのフレーム長が異なり、一方のフレーム内にデータが存在しない部分が生ずる場合でも、情報秘匿に係る情報が漏洩することを防止し得るスクランブル方法に係る。
【０００２】
【従来の技術】図５は従来の通信システムのレイヤ構成（プロトコル・スタック）の例を示す図であって、数字符号６１は上位レイヤのフレーム、６１－ａはヘッダ、６１－ｂは情報フィールド、６２～６４はそれぞれ下位レイヤのフレーム、６２－ａ，６３－ａ，６４－ａはヘッダ、６２－ｂ，６３－ｂ，６４－ｂは情報フィールドを表わしている。
【０００３】また、英字符号Ｂは上位レイヤのフレームの末尾、Ｃは下位レイヤのフレーム６４の情報フィールド６４－ｂで上位レイヤのフレーム６１の情報フィールド６１－ｂの情報が尽きた箇所、Ｄは下位レイヤのフレーム６４の情報フィールド６４－ｂ内で上位レイヤからの情報が存在しない部分を表わしている。

2

【０００４】従来、図５に示すように、複数レイヤから構成される通信システムにおいて、上位レイヤのフレームサイズが下位レイヤの１フレームに含まれるデータ長の倍数になっていない場合には、上位レイヤのフレーム末尾Ｃを含む下位レイヤのフレーム６４の上位レイヤのフレームの末尾に対応する箇所Ｃ以降のＤで示す部分に０を埋め込んでいた。
【０００５】また、複数レイヤ構成をとらない通信システムにおいても、ユーザが送りたいデータの長さが、１フレームに含まれるデータ長の倍数になっていない場合には上記の場合と同様に、データ末尾以降の部分に０を埋め込んでいた。
【０００６】このように、フレーム末尾を空白コードで埋め込むシステムの１つに、ＲＣＲＳＴＤ－６で規定されている、「陸上移動無線データ通信を行う無線局の無線設備」（１９９０年１月２５日策定）がある。
【０００７】
【発明が解決しようとする課題】伝送するデータについて情報を秘匿する方法として、２値（“１”，“０”）の擬似乱数を発生し、データとの排他的論理和を計算して送信し、受信側では、同じ系列の疑似乱数列を発生することにより復号を行なう方式が採られることが多い。
【０００８】前述したような送受信間で一方のフレーム長が他方のフレームの情報フィールドの整数倍になっていないような条件では一方のデータフレームの末尾に一定周期あるいは毎回、データとして“０”の列が組み込まれているので、この箇所では、前述のような情報秘匿のためのスクランブルをかけるとスクランブルパターンと“０”の排他的論理和、すなわち、スクランブルパターン（擬似乱数）そのものが伝送路に送出されることになる。
【０００９】図６はスクランブルパターン発生器の例を示す図である。同図において、６５－１～６５－１０はレジスタ、６６は排他的論理和回路を示している。
【００１０】スクランブルによる情報秘匿を行なうシステムでは、同図に示すようなスクランブルパターン発生器（線形フィードバック・シフト・レジスタで構成される）を用いて、レジスタ６５－１～６５－１０（１つが１ビットのデータを格納する）に、端末の秘密ＩＤなどをセットし、１サイクルごとに、レジスタの値を右へ１つずつシフトし、右端のレジスタから１ビットずつ出力し、左端には３ビット目と１０ビット目の排他的論理和を入力する。
【００１１】スクランブルパターン発生器のビット数をｍとすると、スクランブルパターン発生器の構造がわかっていなければ、２ｍビット分、スクランブルパターン発生器の構造が分かっていれば、ｍビット分の疑似乱数が分かれば、初期値レジスタの値を連立方程式を解くこ

とにより逆算できる。mの値の１例として、簡易型携帯電話標準規格（ＲＣＲ　ＳＴＤ－２８）では１０ビット用いること、と定めている。

【００１２】そのため、条件によってはスクランブルパターンの内容からスクランブルパターン発生器の初期値レジスタの値を第三者に推定される可能性があると言う好ましくない問題が予想される所であった。

【００１３】本発明は、このような従来の課題を解決するために成されたものであって、送信側のフィールド長と受信側の情報フィールド長（または受信側の情報フィールド長の和）とが等しくない場合であっても、外部からスクランブルパターンを解読することが不可能なスクランブル方法を提供することを目的としている。

【００１４】

【課題を解決するための手段】本発明によれば、上述の課題は、前記特許請求の範囲に記載した手段により解決される。

【００１５】すなわち、請求項１の発明は、送信すべきデータＡを固定長のバケットまたはフレーム単位に分割して送受信し、その際スクランブルによる情報秘匿を行なう通信方法において、前記データＡの末尾のビットを含むバケットまたはフレームが、１バケットまたは１フレーム分の送信データに満たない場合、前該データＡの末尾以降の部分に擬似乱数列を埋め込んで１バケットまたは１フレーム分の送信データを満たしてからスクランブルをかけるように構成したスクランブル方法である。

【００１６】請求項２の発明は、送信すべきデータＡを固定長のバケットまたはフレーム単位に分割して送受信し、その際スクランブルによる情報秘匿を行なう通信方法において、前記データＡの末尾のビットを含むバケットまたはフレームが、１バケットまたは１フレーム分の送信データに満たない場合、前該データＡの末尾以降の部分に、該データＡの一部分を埋め込んで１バケットまたは１フレーム分の送信データを満たしてからスクランブルをかけるように構成したスクランブル方法である。

【００１７】請求項３の発明は、送信すべきデータＡを固定長のバケットまたはフレーム単位に分割して送受信し、その際スクランブルによる情報秘匿を行なう通信方法において、前記データＡの末尾のビットを含むバケットまたはフレームが、１バケットまたは１フレーム分の送信データに満たない場合、前該データＡの末尾以降の部分に０を埋め込んで１バケットまたは１フレーム分の送信データを満たすと共に、該バケットまたはフレーム内のデータの先頭からデータＡの末尾までの部分についてスクランブルをかけるように構成したスクランブル方法である。

【００１８】

【作用】本発明は、データを固定長のバケット、または、フレーム単位に分割して送受信し、その際スクランブルによる情報秘匿を行なうように構成された通信系において、伝送データから情報秘匿のためのスクランブルパターンが第三者に解読されないようにしたものである。



【００１９】請求項１の発明では、データ長と、バケットまたはフレーム長の差から生じた空白部に疑似乱数列を埋め込んでいる。従来はこの空白部を“０”で満たしていたため、“０”とスクランブルパターンの各ビットとの排他的論理和を採ることによりスクランブルをかけていた。

【００２０】そのため、スクランブルパターンそのものが伝送されてしまう結果を生じていたが、このように疑似乱数列を埋め込むことによりスクランブルパターンそのものが表われることがなくなるから、第三者によって、伝送データからスクランブルパターンを解読されることを防止できる。従って、スクランブルパターン発生器の初期値レジスタの内容が推定されることもない。

【００２１】また、請求項２の発明では、バケットまたはフレーム内の空白部を疑似乱数ではなく、データの一部を用いて埋め込んでいる。従って、請求項１の場合と同様な理由により、第三者によって、伝送データからスクランブルパターンを解読されることを防止できる。

【００２２】更に、請求項３の発明では、バケットまたはフレーム内の空白部を“０”あるいは任意のデータで満たすが、この部分を除いてスクランブルをかけるようにしている。この方法によってもスクランブルパターンの各ビットと“０”との排他的論理和を採って出力するということがなくなるのでスクランブルパターンが外に表われることがない。従って、第三者によって、伝送データからスクランブルパターンを解読されることを防止できる。

【００２３】

【実施例】図１は本発明の第１の実施例を説明する図であって、数字符号１はプロトコル制御部、２，７はスクランブルパターン発生器、３は疑似乱数発生器、４，５はバッファ、６は排他的論理和回路、８は送信データ、９，９ａはヘッダ、１０，１０ａはフレーム長情報のフィールド、１１，１１ａは情報フィールド、１２は受信データ、１３は送信側で付加された疑似乱数列を表わしている。

【００２４】同図に示すように、送信側では、ユーザまたは上位レイヤから送信要求のあったデータ８は一旦バッファ４に蓄えられ、プロトコル制御部１が、１回分の送信データずつ取り出して、スクランブルパターン発生器２により生成されたビット列との排他的論理和を演算して送信する。

【００２５】送信データ８の残りデータが、１フレームまたは１バケット分の送信データに満たない場合は、疑似乱数発生器３から送られてくる疑似乱数のビット列で最後のフレームまたはバケットの、余った部分を埋める。

5

【００２６】受信側では送られてきたデータ１２を順次バッファ（図示せず）に蓄えていき、フレーム長を表わすフィールド１０ａを見て、必要部分だけ切り出してバッファ５に移し、スクランブルパターン発生器７により生成したビット列との排他的論理和を演算して出力する。

【００２７】図２は本発明の第２の実施例を説明する図であって、数字符号については、先に説明した図１の場合と同様である。また受信側の構成は図１の場合と概ね同様であるので本図では送信側のみ示している。

【００２８】同図において、ユーザまたは上位レイヤから送信要求のあったデータ８は、一旦バッファ４に蓄えられ、プロトコル制御部１が、１回分の送信データずつ取り出して、スクランブルパターン発生器２により生成されたビット列との排他的論理和を演算して送信する。

【００２９】このとき、送信データ８の残りデータが、１フレームまたは１パケット分の送信データに満たない場合は、送信データ８の最終ビットが含まれるフレームまたはパケットの当該ビット以降の領域Ｆに、送信データ８の末尾の必要な長さのビット列Ｅを複製して埋め込み、スクランブルパターン発生器２により生成されたビット列との排他的論理和を演算して、伝送路上に送出する。

【００３０】図３は本発明の第３の実施例を説明する図であって、数字符号については、先に説明した図１の場合と同様である。また、受信側の構成は図１の場合と概ね同様であるので、本図では送信側のみ示している。

【００３１】同図において、ユーザまたは上位レイヤから送信要求のあったデータ８は、一旦バッファ４に蓄えられ、プロトコル制御部１が１回分の送信データずつ取り出して、スクランブルパターン発生器２により生成されたビット列との排他的論理和を演算して送信する。

【００３２】バッファ４の残りデータが、１フレームまたは１パケット分の送信データに満たない場合は、送信側は、ユーザまたは上位レイヤから送信要求のあったデータ８中のフレーム長を表わすフィールド１０を見て、必要数だけのビット列をスクランブルパターン発生器２に発生させ、最後のフレームまたはパケットの、余った部分にはスクランブル処理を行なわず、“０”を埋め込んで伝送路に送出する。この実施例の場合には、埋め込むデータは“オール０”である必要はなく任意の文字列であって良い。

【００３３】図４は簡易型携帯電話標準規格（ＲＣＲＳＴＤ－２８）に準拠したプロトコルの例を示す図である。同図において、数字符号１４はパーソナルステーション（ＰＳ）、１５はセルステーション（ＣＳ）、１６はネットワーク（網）を示している。

【００３４】この規格に準拠してパケット通信を行なう場合には、課金を行なう必要から、同図のように、データの送達確認のため、ｅｎｄ　ｔｏ　ｅｎｄで終端される。ＬＡＰＤ（Ｌｉｎｋ　Ａｃｃｅｓｓ　Ｐｒｏｃｅｄｕｒｅ　ｏｎ　ｔｈｅ　Ｄ－ｃｈａｎｎｅｌ）レイヤを、携帯端末－無線基地局間で終端される、ＬＡＰＤＣ（Ｌｉｎｋ　Ａｃｃｅｓｓ　Ｐｒｏｃｅｄｕｒｅ　ｆｏｒ　Ｄｉｇｉｔａｌ　Ｃｏｒｄｌｅｓｓ）レイヤの上に置くプロトコル構成が考えられる。

6

【００３５】この構成において、複数のＬＡＰＤフレームに渡るデータ送信要求が発生した場合、ＬＡＰＤフレーム（情報フィールド最大２６０オクテット＋制御部５／６オクテット＝２１２０／２１２８ビット）をＬＡＰＤＣフレーム（２０オクテット＝１６０ビット）に分割して送受するため、余りの１５／１４バイト＝１２０／１１２ビットについては従来の技術で説明したような、空白ビットを“０”で埋める手順が行なわれる。

【００３６】このように、現実の通信システムにおいて、２０ビット以上のビット列に対して、従来の技術で説明したような、空白ビットを“０”で埋める手順が行なわれる場合は多く存在し、そのような場合に、本発明を適用して、スクランブルパターンがそのまま伝送路に送出されないようにすることによって、情報秘匿の信頼性を高めることができる。

【００３７】

【発明の効果】以上説明したように、本発明によれば、送信すべきデータを固定長のパケットまたはフレーム単位に分割して送受信し、その際、スクランブルによる情報秘匿を行なう通信系において、送信すべきデータの末尾のビットを含むパケットまたはフレームが、１パケットまたは１フレーム分の送信データに満たない場合に、該送信データの末尾以降のビット列からスクランブルパターンを検出することを防止できるので、第三者によってスクランブルパターン発生器の初期値レジスタの値を推定されるという恐れをなくし、確実な情報秘匿を行なうことができる利点がある。

【図面の簡単な説明】

【図１】本発明の第１の実施例を説明する図である。

【図２】本発明の第２の実施例を説明する図である。

【図３】本発明の第３の実施例を説明する図である。

【図４】簡易型携帯電話標準規格に準拠したパケット通信のプロトコル構成の例を示す図である。

【図５】従来の通信システムのレイヤ構成の例を示す図である。

【図６】スクランブルパターン発生器の例を示す図である。

【符号の説明】

１　　プロトコル制御部

２，７　　スクランブルパターン発生器

３　　疑似乱数発生器

４，５　　バッファ

６　　排他的論理和回路

８　　送信データ

7

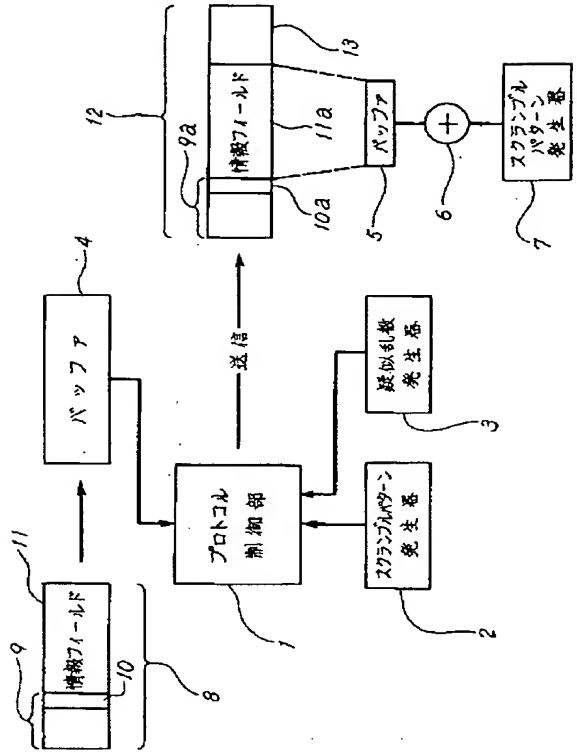
９，９ａ　ヘッダ
１０，１０ａ　フレーム長情報のフィールド
１１，１１ａ　情報フィールド
１２　受信データ

8

＊１３　送信側で付加された疑似乱数列
１４　パーソナルステーション
１５　セルステーション
＊　１６　ネットワーク

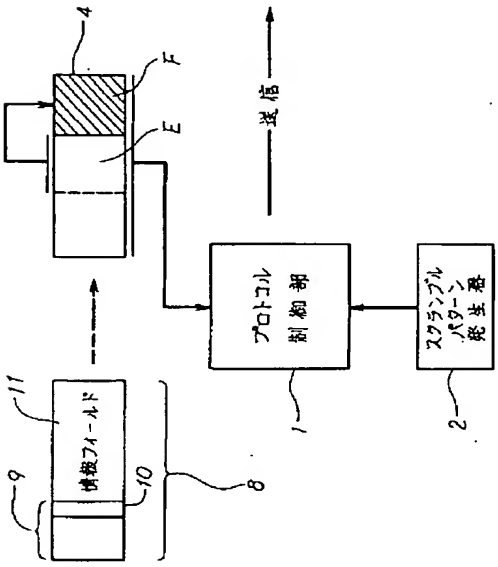
【図１】

本発明の第１の実施例を説明する図



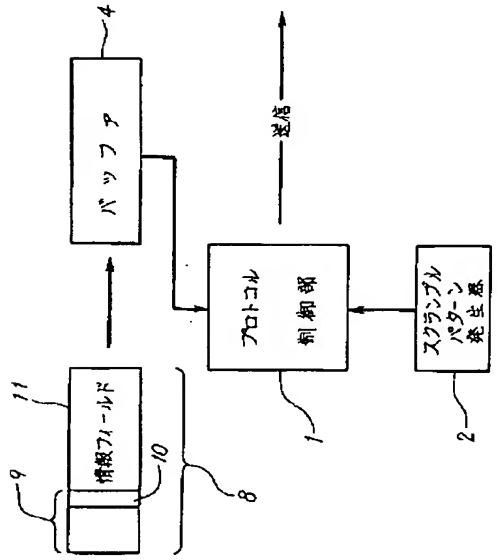

【図２】

本発明の第２の実施例を説明する図



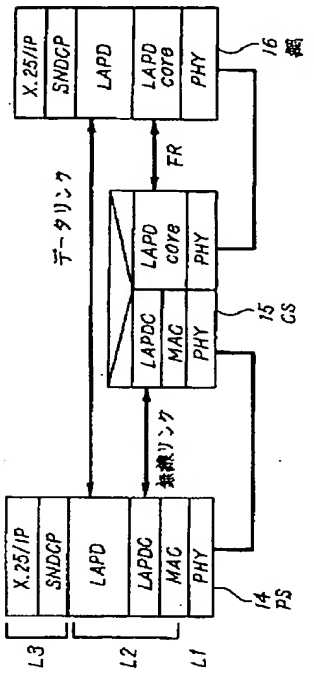

【図３】

本発明の第３の実施例を説明する図



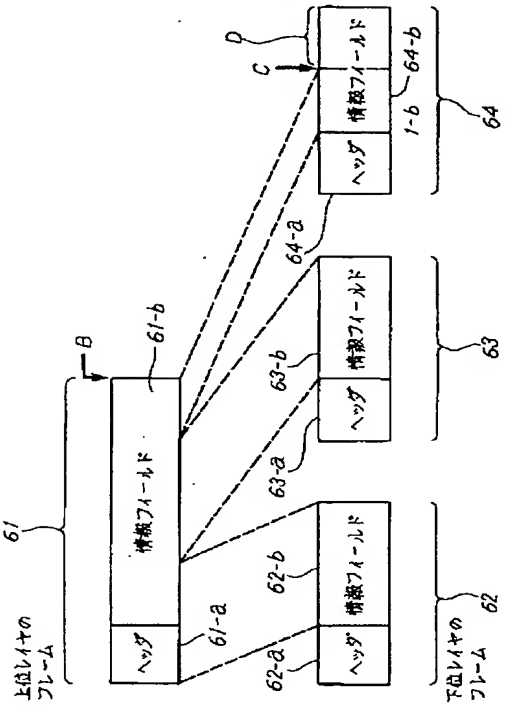
【図４】

RCR STD-28に準拠したパケット通信のプロトコル構成の例を示す図




【図５】

従来の通信システムのレイヤ構成の例を示す図



【図６】

スクランブルパターン発生器の例を示す図